Cabinet for Health and Family Services
Division of Kentucky Electronic Health Information

Policies – Information Technology

Category: 15 000.000
Category Title: DIVISION OF KENTUCKY ELECTRONIC HEALTH INFORMATION OBLIGATIONS: Privacy

000.000 Policy Title: Notice of Privacy Breach

Policy: Notice of Privacy Breach: The Division of Kentucky Electronic Health Information and KHIE personnel and contractors will maintain the privacy and security of protected health information (PHI) consistent with The Division of Kentucky Electronic Health Information policies and all applicable laws and regulations. The Division of Kentucky Electronic Health Information follows HIPAA requirements for logging security incidents. Additionally, the Division of Kentucky Electronic Health Information investigates potential security breaches, as defined under HITECH, and complies with all reporting requirements, as outlined under the HITECH Act.

Any the Division of Kentucky Electronic Health Information and KHIE personnel and contractors who suspect an information security incident must report the incident to their supervisor within 1 hour of discovery. CHFS IT follows a controlled process to log, investigate, and report all security incidents. The Division of Kentucky Electronic Health Information adheres to this procedure and all federal requirements regarding the investigation, management, and reporting of information regarding security incidents and/or security breaches.

The Division of Kentucky Electronic Health Information will notify the Participant of potential HIPAA violations consistent with the requirements of this policy and according to the Business Associates Agreement between the Division of Kentucky Electronic Health Information and Participant.

1.1 Definition of "Breach": The term "Breach" means the unauthorized acquisition, access, use, or disclosure of PHI which compromises, i.e., poses a significant risk of financial, reputational or other harm to the individual, the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.

1.1.2 The term "Breach" does not include:

(a) Any unintentional acquisition, access, or use of PHI by an employee or individual acting under the authority of the Division of Kentucky Electronic Health Information or a Business Associate if:

(i) such acquisition, access, or use was made in good faith and within the course and scope of the employment or other professional relationship of such employee or

(ii) individual, respectively, with the Division of Kentucky Electronic Health Information or a Business Associate; and such information is not further acquired, accessed, used, or disclosed by any person; or

(b) Any inadvertent disclosure from an individual who is otherwise authorized to access PHI at the KHIE facility operated by the Division of Kentucky Electronic Health Information or a Business Associate to another similarly situated individual at the same facility; and

(c) Any such information received as a result of such disclosure is not further acquired, accessed, used or disclosed by any person without patient authorization.

1.2 "Secured PHI" is rendered unusable, unreadable and indecipherable; thus, the Division of Kentucky Electronic Health Information will establish a breach notification process applicable to "Unsecured PHI".

1.3 "Unsecured PHI" is PHI that is not:

- secured by a technology standard that renders PHI unusable, unreadable, or indecipherable to unauthorized individuals or
- secured by a technology that is developed or endorsed by a standards developing organization accredited by the American National Standards Institute.

1.4 In the event the Division of Kentucky Electronic Health Information discovers a breach of Unsecured PHI, the Division of Kentucky Electronic Health Information will notify:

(a) each Participant entity whose Unsecured PHI has been, or is reasonably believed by the Division of Kentucky Electronic Health Information to have been accessed, acquired, or disclosed as a result of such breach.

(b) The notification requirement applies to any Unsecured PHI accessed, maintained, retained, modified, recorded, stored, destroyed, or otherwise held, used or disclosed by the Division of Kentucky Electronic Health Information. The notification requirements also apply to breaches committed by the Division of Kentucky Electronic Health Information or one of its Business Associates.

1.5 For purposes of this Policy, a Breach will be treated as discovered by the Division of Kentucky Electronic Health Information or one of its Business Associates as of the first day on which the Breach is known to the Division of Kentucky Electronic Health Information or one of its Business Associates, respectively, (including any person, other than the individual committing the breach, that is an employee, officer, or agent of the Division of Kentucky Electronic Health Information or one of its Business Associates, respectively or should reasonably have known to the Division of Kentucky Electronic Health Information or one of its Business Associates to have occurred.

(a) Whether a Breach compromises the privacy or security of PHI, the Division of Kentucky Electronic Health Information will perform a risk assessment to evaluate:

(i) the nature of data elements breached,

(ii) the likelihood that the PHI is accessible and useable by unauthorized persons;

(iii) what physical, technical, and procedural safeguards were employed by the Division of Kentucky Electronic Health Information;

(iv) whether the PHI is at a low, moderate, or high risk of being compromised;

(v) the likelihood that unauthorized individuals will know the value of the information and use or sell it;

(vi) the level of potential harm:

- Broad reach of potential harm (blackmail, disclosure of private facts, disclosure of sensitive PHI, mental pain and emotional distress, address information for victims of abuse, humiliation, identity theft).
- Likelihood harm will occur (which depends on manner of actual breach and types of data such as SS#, passwords, mother's maiden name, and information useful for identity theft).
- If identity theft or fraud is a risk, review and consider purchasing theft identity insurance for individuals.
- The Division of Kentucky Electronic Health Information's ability to mitigate risk of harm and contain the breach, including consideration of appropriate counter-measure, such as monitoring systems for misuse of the PHI and monitoring for patterns of suspicious behavior that the Division of Kentucky Electronic Health Information can implement.

1.6 The Division of Kentucky Electronic Health Information's Executive Director shall document the process and results of any Risk Assessment. The Executive Director shall retain such forms for at least a six-year period in accordance with CHFS's Document Retention Policy.

Scope: This policy applies to all Division of Kentucky Electronic Health Information and KHIE employees and contractors, including all persons providing contractor services.

Policy/Procedure Maintenance Responsibility: The Division of Kentucky Electronic Health Information is responsible for the maintenance of this policy.

Exceptions: There are no exceptions to this policy.

Review Cycle: Bi-Annual

Timeline:
Revision Date:
Review Date: 01-16-2017
Effective Date: 06-15-2011